WO0017758

Title:
SECURE DATA ENTRY PERIPHERAL DEVICE

Abstract:

A secure data entry peripheral device in a computer system featuring an encryption technique integrated within the device itself, and not by other means, so that each transmission of data from the peripheral device is already encrypted, giving it a high level of security with its initial transmission. Encryption on the proposed single chip microprocessor is completely secure because the "Keyboard", "Data entry" or "Analog voice" encoding and encryption are on the same chip by storing encryption keys and secure data in EEPROM memory (31). There is no opportunity for external interference, which could compromise the integrity of the data enabling maintenance of a high security level. The device can be applied to a keyboard, computer mouse or voice recognition circuit used as data entry devices. Since each device utilizes a microcontroller (25) in its standard configuration, the encryption technique of the present invention can be applied easily and efficiently.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14 — A1

(11) International Publication Number: **WO 00/17758**

(43) International Publication Date: 30 March 2000 (30.03.00)

(21) International Application Number: PCT/IL99/00504

(22) International Filing Date: 16 September 1999 (16.09.99)

(30) Priority Data:
126259 17 September 1998 (17.09.98) IL

(71)(72) Applicant and Inventor: REDLER, Yeshayahu [IL/IL]; Rehov HaTapuach 2, P.O. Box 916, 42815 Pardesia (IL).

(74) Agent: LANGER, Edward; P.O. Box 410, 43103 Raanana (IL).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

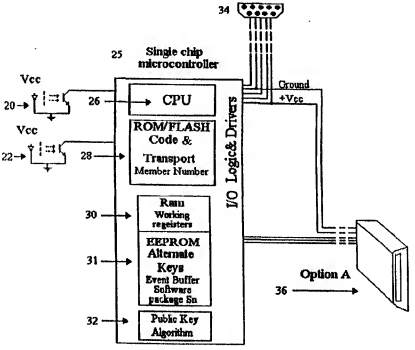
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE DATA ENTRY PERIPHERAL DEVICE

(57) Abstract

A secure data entry peripheral device in a computer system featuring an encryption technique integrated within the device itself, and not by other means, so that each transmission of data from the peripheral device is already encrypted, giving it a high level of security with its initial transmission. Encryption on the proposed single chip microprocessor is completely secure because the "Keyboard", "Data entry" or "Analog voice" encoding and encryption are on the same chip by storing encryption keys and secure data in EEPROM memory (31). There is no opportunity for external interference, which could compromise the integrity of the data enabling maintenance of a high security level. The device can be applied to a keyboard, computer mouse or voice recognition circuit used as data entry devices. Since each device utilizes a microcontroller (25) in its standard configuration, the encryption technique of the present invention can be applied easily and efficiently.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SECURE DATA ENTRY PERIPHERAL DEVICE

FIELD OF THE INVENTION

The present invention relates to data entry peripheral devices such as keyboards, computer mouse pointing devices, voice recognition devices and the like, and more particularly, to an encryption system applied directly in the data entry peripheral device for insuring secure data transmission, including transactional and credit card information, and for preventing unauthorized copying and use of software programs or packages.

BACKGROUND OF THE INVENTION

The rise of the Internet data highway has dramatically increased the need for secure data transmission, to enable a tried and true basis for electronic funds and other secret data transfer and consumer purchase transactions. Credit card information, banking account numbers and other sensitive data are vulnerable to unauthorized use when placed on a data communications network, hence the need for secure transactions. The expected rise in the number of Internet transactions of this type will reach a value of $300 billion in the near future, and the electronic Internet servers and all of the associated data processing equipment need to adapt to this new approach to financial and secure data transactions.

Another related problem is presented by unauthorized copying or use of software programs or packages, which creates heavy software industry losses.

There are known methods and apparatus for providing security in data communications including data encryption techniques, also known as information integrity technology, 'fire-walls' and others. Many examples of this technology exist, such as encryption/decryption, digital signature, certificate authentication, etc. and

there are even computer keyboard-related techniques which are described, for example, in US Patents 5,748,888 to Angelo et al, and 5, 406,624 to Tulpan.

The Angelo patent discloses secure keyboard communications in a computer system. A request for private keyboard communications generates a secure system management interrupt, which directs specialized hardware to intercept and divert keyboard interrupts so that keyboard data is communicated only to a black-box security device controlling access to protected system resources, thereby protecting keyboard data from interception by malicious software.

The Tulpan patent discloses a processor unit connectable between a keyboard and a computer, which enables data to be transmitted to the computer in selected fashion, either via a transparent mode or via one of a plurality of special handling modes. In the transparent mode, the keyboard data passes without any change being made in the data, and in the special handling mode, a security program is executed while secret data inputted via the keyboard data is isolated from the computer.

As described above, a tremendous increase is expected in the number and types of data transactions requiring high levels of security for the mass market of on-line purchasers and Internet users. In order to achieve such high rates of growth in this application, the level of sophistication of the user must also increase, so that the operation of secure data transactions is a familiar and acceptable activity. In the patents listed above, the devices utilized are add-on units which may not present user-friendly approaches to achieving secure data transactions, due to complications in software and hardware installation and operation.

It would be desirable, therefore, to provide methods and apparatus which are user-friendly for enabling quick, simple and easy initiation and completion of

secure data transactions with a high degree of user confidence in the security level, and preventing unauthorized copying and use of software programs and packages.

SUMMARY OF THE INVENTION

Accordingly, it is a principal object of the present invention to overcome the disadvantages of prior art techniques used in secure data transactions, by providing a quick, simple and easy to use method of insuring a high level of security in such transactions, using a specially-designed keyboard, computer mouse, or voice recognition circuit.

In accordance with a preferred embodiment of the present invention, there is provided a secure data entry peripheral device in a computer system, said device comprising:

means for at least one of entry, collection and reading of data information;

controller means for encoding said data information for presentation to the computer system, and

means associated with said controller for processing said encoded data information by performing thereon at least one operation amongst operations including encryption, decryption, data manipulation and non-volatile storage,

said processed encoded data information providing a secure transaction when transmitted within the computer system, and when decrypted and decoded for use at a remote location.

In the preferred embodiment, the inventive secure data entry peripheral device encryption technique is integrated within the device itself, and is not carried out separately on the computer unit or devices attached by wires or add on software

programs, so that each transmission of data from the peripheral device is already encrypted, giving it a high level of security with its initial transmission from the device.

Encryption of data on the proposed single chip microprocessor is completely secure because the 'Key board', 'Data entry' or 'Analog voice' encoding and encryption are on the same chip by storage of encryption keys and secure data in EEPROM memory. There is no external access or opportunity for external interference which could compromise the integrity of the data. This approach enables maintenance of a high security level.

The inventive device can be applied to a keyboard, computer mouse or voice recognition circuit which are used as data entry devices. Since each device utilizes an electronics board or microcontroller in its standard configuration, the encryption technique of the present invention can be applied easily and efficiently, raising the security level of the design.

The inventive device may also employ a contact or contactless Smartcard adaptor to enhance the total security of the system.

Other features and advantages of the invention will become apparent from the following drawings and description.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the invention with regard to the embodiments thereof, reference is made to the accompanying drawings, in which like numerals designate corresponding elements or sections throughout, and in which:

Fig. 1 is an overall plan view of a secure computer mouse peripheral device constructed and operated in accordance with the principles of the present invention;

Fig. 2 is an electronic block diagram of a secure computer mouse

microcontroller included in the Fig. 1 computer mouse peripheral device;

Fig. 3 is an overall view of a secure keyboard peripheral device constructed and operated in accordance with the principles of the present invention;

Fig. 4 is an electronic block diagram of a secure keyboard microcontroller included in the Fig. 3 peripheral device;

Fig. 5 is an electronic block diagram of a secure voice recognition peripheral device constructed in accordance with the principles of the present invention;

Figs. 6a-b show a flowchart describing a typical purchase transaction using the secure I/O device of the present invention; and

Fig. 7 is a flowchart of an authentication routine used in the purchase transaction of Figs. 6a-b.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description of secure data entry peripheral devices in a computer system, the term "secure" is used to describe secure devices such as 'Smart card' or 'Secure Integrated circuit' or 'Electronic coin' or other secured components.

Referring now to Fig. 1, there is shown an overall plan view of a secure computer mouse peripheral device 10 constructed and operated in accordance with the principles of the present invention. Computer mouse device 10 has a microcontroller or an independent logic system which reads optical signals and sends pulses in an asynchronous serial RS 232 format to a serial communication channel via cable 11, or via a computer mouse interface connected directly into the bus of a computer. Thus, the following description applies to computer mouse communications either via a serial communications port or a card inserted into the

computer bus. The reference to a secure mouse includes similar devices such as a track ball or pad or any other computer pointing device in one, two or more dimensions.

Normally, data communications with the secure computer mouse 10 are performed by a service program running on the computer. The present invention enables entry of data by selection of numbers and values which are presented to the user on the computer screen. The selected numbers and values have a secret content or a monetary value, and are sent back by the secure computer mouse 10 as encrypted data after a special command is sent from the computer service program to the secure computer mouse 10, or the command is entered by an external signal like one of the mouse keys. This special command is decoded by secure computer mouse 10 and the data to which computer mouse 10 already points is encrypted directly by the microcontroller associated with the secure computer mouse 10.

Alternatively, when the program running on the computer issues a special command as follows: encrypt / decrypt data which follows the command, then this command is interpreted directly by the microcontroller associated with the secure computer mouse 10, thus giving it a high security level.

Alternatively, in order to increase the level of security the numbers and values can be entered by an optional mini-keypad 16 on computer mouse 10.

In this fashion, the encryption unit in secure computer mouse 10 is an acceptable unit to a wide cross-section of computer users. The security level of data encrypted in this fashion is the highest possible since no code or system encryption key is run on the computer service program or stored on the computer disk.

The secure computer mouse 10 can provide various levels of encryption and security. In addition to the standard computer mouse operating

software, a large number of encryption/decryption programs are provided. Those encryption/decryption programs are uniform in every type of secure computer mouse 10, and includes various encryption algorithms, such as standard DES (data encryption standard) functions, 3-DES, RC2-RCn, IDEA, HASH, CAST, a dynamic exchange of system encryption keys, and public key technology such as RSA algorithms, Diffie-Hellman, etc.

Each secure computer mouse 10 has a 'member number' permanently encoded in it, which remains even if the encryption keys are changed. The permanent encoding of a private key, a public (RSA) algorithm seed, Key1 and Key2 of a 3-DES algorithm can be achieved by automatic encoding, without human intervention so that complete security is insured while keeping a user friendly environment

The 'member number' is a silicon file containing tens of characters. The 'member number' contains the default value of the encryption keys, personal identification number (PIN), attribute codes and control and rescue code. By a special procedure involving the PIN number, the user can change the DES keys and public and private keys as well.

In accordance with the invention, there are two available levels of security for secure computer mouse device 10, Level I and Level II.

In Level I, secure computer mouse 10 enables entry of data by selection of numbers and values which are presented to the user on the computer screen. Alternatively, the data can be entered by optional mini-keypad 16 on secure computer mouse 10 and stored in an EEPROM memory/Smartcard component integrated within the device. These numbers and data values are encrypted by various methods, including, DES or 3-DES, RC2-RCn, IDEA, HASH, CAST, a dynamic exchange of

system encryption keys, and public key technology such as RSA algorithms, Diffie-Hellman, etc. There is no access to the system key which is permanently encoded in the microcontroller of secure computer mouse 10.There is also no access to the 'member number' permanently encoded in the microcontroller of secure computer mouse 10.

To obtain a secure I/O communication link from secure computer mouse 10, a secure I/O negotiation begins with a bi-directional authentication routine. Once this is achieved, the data which is entered via the secure computer mouse 10 is then encrypted and can be sent directly or via the secure I/O communication link to a service provider, at a remote location. The Level I security level is intended for purchases via the Internet, involving relatively small sums.

In the Level II security level, the secure computer mouse 10 is constructed with a 'Smartcard' interface 12, typically located on the lower section of the mouse housing. This arrangement will enable both Levels I and II to be performed. Alternatively, the construction may be one having a Smartcard component as an integral part of the secure computer mouse 10 device, using a monolithic or hybrid chip construction, as shown in Fig. 2. An encryption/decryption routine can be used which integrates the microcontroller in secure computer mouse 10, with a 'Smartcard' security (encryption/decryption) algorithm, and this integration greatly enhances the overall security of the secure computer mouse 10.

Integration of the secure computer mouse 10 microcontroller and the 'Smartcard' security (encryption/decryption) algorithm enables secure computer mouse 10 to continually adopt new security methodologies and encryption/decryption algorithms, which are provided on the 'Smartcard' 14.

The Level II security level makes it possible for banking institutions, which require a high level of security for transfer of encrypted data and files, to handle electronic transfer of large sums of money as well as transfers between them.

The advantage of using a secure computer mouse 10 for encryption of data is that it is extremely easy, since the user is accustomed to performing computer operations via the computer mouse. Thus, practically no training or explanation is needed in use of secure computer mouse 10, and the classification of computers and new models generally does not affect the operation of the secure computer mouse device 10.

If a change is to be made in the system encryption key, due to a breach in system security, this can be performed by transmission of new system encryption keys coded by a public key algorithm. It is possible to arrange a plurality of system encryption keys which can be automatically replaced on a regular basis in relation to the time of day, or the date.

The Level II security level can be applied to prevent unauthorized use of software programs or packages, by use of the secure computer mouse 10, with the addition of a Smartcard by the manufacturer of the software product. The software package serial number is encrypted onto the Smartcard, which is inserted into the Smartcard interface 12, and when decrypted, the software is enabled.

The Level II secure computer mouse 10 achieves better security in an easier fashion than the security plugs now typically used as an attachment device to a keyboard or printer interface.

The secure computer mouse 10 may be applied in all environments, including banks and commercial entities, so that their data processing systems have the system encryption key stored in the computer mouse. In this way, the

system encryption key is not kept or stored on any disk, or in the computer memory, where it may be exposed to illegal tampering or attempts to breach security.

Referring now to Fig. 2, there is shown an electronic block diagram of a secure computer mouse microcontroller 25 included in the Fig. 1 mouse peripheral device 10. A pair of position optical encoders 20, 22 feed position information provided by the mouse trackball as input to the mouse microcontroller 25.

Microcontroller 25 can be implemented in accordance with skill of the art electronic design techniques, and comprises functional blocks including a CPU 26, flash memory or EEPROM 28 containing code and default (transport) 'member number' value Microcontroller 25 also comprises RAM working registers 30, and EEPROM data storage memory 31, which will hold alternate encryption keys, a software package serial number, and historical transaction buffer, which records the last 10 transactions, for example, on the EEPROM memory 31, to resolve billing disputes. Microcontroller 25 also comprises public key algorithm 32. Mouse device 10 is connected via an RS-232 connector 34 for serial communication with the host computer, or it may be connected via the mouse interface card directly to the computer bus.

As shown in Option A, a 'Smartcard' adapter 36 may be added to the system to provide for operation with system encryption keys encoded on the Smartcard 14, or with a Smartcard PIN number or Smartcard security algorithm.

In Fig. 3 there is shown an overall view of a secure keyboard peripheral device 40 constructed and operated in accordance with the principles of the present invention.

Keyboard 40 has a stand-alone microcontroller having an embedded code and is connected via cable 41 to a keyboard interface in the computer. In

accordance with the principles of the present invention, a standard keyboard can be replaced by a secure keyboard 40 having a high security level. Keyboard 40 features an optional magnetic card reader 42 and an optional Smartcard interface 44, operating as described further herein.

Normally, data communications with the secure keyboard 40 are performed by a service program running on the computer. The present invention enables entry via secure keyboard 40 of data containing numbers and values, which have a secret content or a monetary value, and this data is entered directly via secure keyboard 40. Thus, the data is sent already encrypted directly by the microcontroller associated with the secure keyboard 40, giving it a high security level. In this fashion, the encryption unit in secure keyboard 40 is the unit that performs keyboard encoding. The security level of data encrypted in this fashion is the highest possible since no code or system encryption key is run on the computer.

Secure keyboard 40 can provide, with a different encryption key, the decryption of data sent to it by the computer, for purposes of authentication, etc. The secure keyboard 40 can provide various levels of encryption and security. In addition to the standard keyboard operating software, an encryption program is provided. The encryption program is uniform in every type of secure keyboard 40, and these numbers and data values are encrypted by various methods, including, DES or 3-DES, RC2-RCn, IDEA, HASH, CAST, a dynamic exchange of system encryption keys, and public key technology such as RSA algorithms, Diffie-Hellman, etc. There is no access to the system key which is permanently encoded in the microcontroller of secure keyboard 40. There is also no access to the 'member number' permanently encoded in the microcontroller of secure keyboard 40.

To obtain a secure I/O communication link from secure keyboard 40,

a secure I/O negotiation begins with a bi-directional authentication routine. Once this is achieved, the data which is entered via the secure keyboard 40 is then encrypted and can be sent directly or via the secure I/O communication link to a service provider, at a remote location. Each secure keyboard 40 has a 'member number' permanently encoded in it, which remains even if the encryption keys are changed.

The permanent encoding of a private key, a public (RSA) algorithm seed, Key1 and Key2 of a 3-DES algorithm can be achieved by automatic encoding, without human intervention so that complete security is insured while keeping a user friendly environment.

The 'member number' is a silicon file containing tens of characters. The 'member number' contains the default value of the encryption keys, personal identification number (PIN), attribute codes and control and rescue codes. By a special procedure involving the PIN number, the user can change the DES keys and public and private keys as well.

In accordance with the invention, there are two available levels of security for secure keyboard device 40, Level I and Level II.

In Level I, secure keyboard 40 enables entry of data containing numbers and values, which have a secret content or a monetary value, and this data is entered directly via secure keyboard 40, and stored in an EEPROM memory/Smartcard component integrated within the device. These numbers and data values are encrypted by various methods, including, DES or 3-DES, RC2-RCn, IDEA, HASH, CAST, a dynamic exchange of system encryption keys, and public key technology such as RSA algorithms, Diffie-Hellman, etc.

The Level I security level is intended for purchases via the Internet, involving relatively small sums.

In the Level II security level, the secure keyboard 40 is constructed with a Smartcard interface 44, typically located on the side of the keyboard housing. This arrangement will enable both Levels I and II to be performed. Alternatively, the construction may be one having a Smartcard component as an integral part of the secure computer mouse 10 device, using a monolithic or hybrid chip construction, as shown in Fig. 4. An encryption routine can be used which integrates the microcontroller in secure keyboard 40, with a Smartcard security (encryption/decryption) algorithm, and this integration greatly enhances the overall security of the secure I/O encryption. Integration of the secure keyboard 40 microcontroller and the Smartcard encryption algorithm enables secure keyboard mouse 40 to continually adopt new security methodologies and encryption/decryption algorithms, which are provided on the Smartcard 14.

The Level II security level makes it possible for banking institutions, which require a high level of security for transfer of encrypted files, to handle electronic transfer of large sums of money and for transfers between them.

The advantage of using a secure keyboard 40 for encryption of data is that it is extremely easy, since the user is accustomed to performing computer operations via the keyboard. Thus, practically no training or explanation is needed in use of secure keyboard 40, and the classification of computers and new models generally does not affect the operation of the keyboard. If a change is to be made in the system encryption key, due to a breach in system security, this can be performed by transmission of new system encryption keys coded by a public key algorithm. It is

possible to arrange a plurality of system encryption keys which can be automatically replaced on a regular basis in relation to the time of day, or the date.

The Level II security level can be applied to prevent unauthorized use of software programs or packages, by use of the secure keyboard 40, with the addition of a Smartcard by the manufacturer of the software product. The software package serial number is encrypted onto the Smartcard, which is inserted into the Smartcard interface 44, and when decrypted, the software is enabled.

The Level II secure keyboard 40 achieves better security in an easier fashion than the security plugs now typically used as an attachment device to a keyboard or printer interface.

The secure keyboard 40 may be applied in all environments, including banks and commercial entities, so that their data processing systems have the system encryption key stored in the secure keyboard 40. In this way, the system encryption key is not kept or stored on any disk, or in the computer memory, where it may be exposed to illegal tampering or attempts to breach security.

Fig. 4 is an electronic block diagram of a secure keyboard microcontroller 45 included in the secure keyboard 40 of Fig. 3. A keyboard matrix of key contacts 53 is fed as input to the keyboard microcontroller 45. Microcontroller 45 comprises functional blocks including a CPU 46, flash memory or EEPROM 48 containing code and default (transport) member number value. Microcontroller 45 also comprises RAM working registers 47, and EEPROM memory 49, with alternate encryption keys, and h'storical transaction buffer, which records the last 10 transactions, for example, on the EEPROM memory 49, to resolve billing disputes. Microcontroller 45 also comprises public key algorithm 50. Secure keyboard 40 is

connected via cable 41 and connector 51 to the keyboard interface for communication with the host computer, or to a universal serial bus interface (USB).

As shown in Option A, a Smartcard adapter 44 may be added to the system to provide for operation with system encryption keys encoded on Smartcard 14, or with a Smartcard PIN number or Smartcard security algorithm

As shown in Option B, a magnetic card reader 42 may be added to the system to provide an easy way of using a credit card number. The magnetic card is used in security Level I or Level II transactions.

Fig. 5 is an electronic block diagram of a secure voice recognition peripheral device 60 constructed in accordance with the principles of the present invention. A secure voice recognition circuit comprises a microphone 62, and a microcontroller 61 which comprises an analog switch 64, A/D converter 66 and D/A converter 68. Microcontroller 61 comprises functional blocks including a CPU 72, a flash memory or EEPROM 74 containing code and default (transport) member number value. Microcontroller 61 also comprises RAM working registers 76, and an EEPROM data memory 78 which holds alternate encryption keys, a software package serial number, and an historical transaction buffer which records the last 10 transactions, to resolve billing disputes. Microcontroller 61 also comprises a public key algorithm 79. A voice signature can also be stored on EEPROM data memory 78.

In operation, audio input is fed from microphone 62 into A/D converter 66, under control of CPU 72, via analog switch 64. When the voice signals are compared in microcontroller 61 with the voice signature stored in EEPROM data memory 78, D/A converter 68 returns the encrypted analog signals to the analog switch 64 which sends the analog encrypted data to an optional speech recognitiion circuit located in the computer running the service program.

The voice recognition circuit enables recognition of numbers and special words by a voice recognition program which is stored in the code memory 74. The voice recognition circuit can be part of a device containing a large number of voice recognition programs, and may be operated as a stand-alone device to obtain already recognized numbers and transmit an encrypted number. The voice recognition circuit can be part of the new model of keyboards or part of speech add-on recognition cards, or part of voice recognition circuits installed on motherboard computer circuits.

As shown in Option A, a Smartcard adapter 70 may be added to the system to provide for operation with system encryption keys encoded on Smartcard 14, or with a Smartcard PIN number or Smartcard security algorithm

In order to provide each of the secure I/O peripheral devices, secure computer mouse 10, secure keyboard device 40 or secure voice recognition device 60, with security via encryption algorithms, it is first necessary to perform a secure I/O protocol which is designed to prevent the presentation of many keys in a short time period.

Generally, secure I/O peripherals have in their own microcontroller all of the necessary memory. Program code is retained in flash code memory 74, and long-term random memory is provided by an EEPROM section in microcontroller 61. The EEPROM memory is electrically erasable and changeable in accordance with the changes in the system encryption keys.

In the manufacturing process of the secure peripherals, an initial member number is written in the microcontroller by the manufacturer. For example, manufacturer A will provide a code having 8 bytes: 00000000, and manufacturer B will provide a code having 8 bytes: 00000001, etc. for as many codes as needed. Using

this encoded key, the manufacturer can check the production line and send the secure peripheral to an encryption center.

In the hardware configuration of the microcontroller, additional hardware is integrated which does not permit more than three authentication routines to be performed in consecutive fashion. After an attempt is made to exceed this number of routines, the system will automatically wait 3 minutes before allowing additional attempts to be made. Each authentication routine is bi-directional. Upon power-on or reset, the system will wait 3 minutes. This automatic system delay is designed to reduce the likelihood of a successful breach of security, by method involving rapid presentation of different system encryption keys.

The inventive secure I/O peripherals include all the existing encryption techniques, including, DES or 3-DES, RC2-RCn, IDEA, HASH, CAST, a dynamic exchange of system encryption keys, and public key technology such as RSA algorithms, Diffie-Hellman, etc. Use of each of these techniques is designed to guarantee the longevity of the system after its initiation into use. Currently, banking encryption systems utilize the DES technique, and most Smartcards do also, except for those used in satellite home communications, TV cable channels and special applications, in which the Smartcards use the Public key RSA algorithm.

The communication system implemented in the secure peripheral I/O system operates according to the following definitions:

1) Complete security for the source of money transferred and for the amount of money, credit card numbers, customer name, bank account numbers etc. transferred by the network.

2) Each provider or receiver of services has a 'member number', or certificate.

3) The 'member number', when broadcast, is always encrypted.

4) In each transaction, part of the 'member number' and the amount of the transaction will be kept secure, by the service provider.

5) The 'member number' is encoded in the secure I/O peripheral memory during the definition process performed by the system manager.

6) The certification authority (CA- governmental, regulatory or service manager) may obtain the 'member number and the amount of the transaction.

7) No party knows the connection between the 'member number' and the true identity of the user.

8) Blockage of user access will be done by the 'member number'.

In Figs. 6a-b there are shown flowcharts describing a typical purchase transaction using the secure I/O device of the present invention. In block 100, the computer connects to the Internet server. In block 102, the computer loads the secure I/O application program. In block 104, the computer loads the Internet surfing program. In block 106, the user enters an Internet having a virtual shopping mall.

In block 108, the user chooses the item to be purchased. In block 110, the vendor secure I/O program starts the negotiation with the user secure I/O program. The secure I/O programs complete the start of the negotiation phase in block 112 by use of an authentication routine (Fig. 7).

The authentication routine of Fig. 7 is an industry standard type, using for example, the DES encryption. The routine begins in block 90 when the service provider sends a start command to the end user which is acknowleged in block 91. The service supplier creates a random number in block 92 , encrypts it in block 93 and transmits it to the end user via the secure I/O peripheral device of the invention The end user secure I/O device decrypts the received random number in block 94. At this stage, the end user secure I/O device generates a new random number in block 95, and transmits the received random number and the generated random number as a packet, encrypted by the same key. The service supplier secure I/O device decrypts the received packet in block 96, and compares the returned random number to the one it

initially generated. If it matches, then the service supplier encrypts the end user random number by the same key and transmits it back to the end user in block 97. The end user decrypts and compares the received random number in block 98 and if it matches in block 99, the authentication routine is sucessfully completed in block 101, and an OK is sent. If the returned random number does not match in block 96 or 99, the authentication routine fails in block 103.

In decision blocks 114a-b of Fig. 6a, the completion of the authentication routine is tested, and the end user is asked to insert his credit card number in block 116. In block 118, the secure I/O device encrypts the credit card number. In block 120, the end user is asked to insert his PIN number, and then in block 122, he is asked to repeat entry of the PIN number.

In block 124, the secure I/O program checks if the PIN number is OK, and in block 126 the secure I/O program encrypts the PIN number. In block 128, the service program running on the computer transmits the encrypted number to the vendor or service supplier (SRS). In block 130, the SRS decrypts the transmitted data, and in decision block 132 the service supplier checks the end user credit card number against credit card blacklist of users whose cards are blocked. If the credit card is OK, in block 134 the service supplier transmits an encrypted receipt to the end user. Block 136 is the end of the typical transaction. Block 138 is the exit of the secure I/O program.

Having described the invention with regard to certain specific embodiments thereof, it is to be understood that the description is not meant as a limitation since further modifications may now suggest themselves to those skilled in the art and it is intended to cover such modifications as fall within the scope of the appended claims.

CLAIMS:

1. A secure data entry peripheral device in a computer system, said device comprising:

means for at least one of entry, collection and reading of data information;

controller means for encoding said data information for presentation to the computer system, and

means associated with said controller for processing said encoded data information by performing thereon at least one operation amongst operations including encryption, decryption, data manipulation and non-volatile storage,

said processed encoded data information providing a secure transaction when transmitted within the computer system, and when decrypted and decoded for use at a remote location.

2. The device of claim 1 configured as a secure mouse device.

3. The device of claim 1 configured as a secure mouse device wherein said processing means comprises an electronic device capable of encrypting/decrypting and storing data.

4. The device of claim 1 configured as a secure mouse device, wherein said processing means comprises an electronic device capable of encrypting/decrypting and storing data received via asynchronous communication means.

5. The device of claim 1 configured as a secure mouse device, wherein said processing means comprises an electronic device capable of encrypting/decrypting and storing data received via computer bus signals transferred through a mouse interface card.

6. The device of claim 1 configured as a secure mouse device having a mini-keypad for entry of data.

7. The device of claim 1 configured as a secure mouse device wherein said controller means is a mouse encoder and said processing means comprises an electronic device capable of encrypting/decrypting and storing data entered via said mouse, and wherein said mouse encoder and said electronic device comprise a single integrated device.

8. The device of claim 7 wherein said single integrated device further comprises a secure command interpreter which operates to manipulate commands.

9. The device of claim 7 wherein said single integrated device is capable of preventing unauthorized use of software programs.

10. The device of claim 1 configured as a secure keyboard device, wherein said controller means is a keyboard encoder and said processing means comprises an electronic device capable of encrypting/decrypting and storing data entered via said keyboard, and wherein said keyboard encoder and said electronic device comprise a single integrated device.

11. The device of claim 10 wherein said single integrated device does not use removable media such as a Smartcard, security token and the like.

12. The device of claim 10 wherein said single integrated device includes an internal EEPROM memory as an integral part of said device, which stores secure information.

13. The device of claim 10 wherein said single integrated device includes secure, protected encryption keys and data as an internal and integral non-removable element.

14. The device of claim 10 wherein said single integrated device further comprises a secure command interpreter which operates to manipulate commands.

15. The device of claim 10 wherein said single integrated device capable of preventing unauthorized use of software programs.

16. The device of claim 1 configured as a secure voice recognition device, wherein said processing means comprises an electronic device capable of encrypting/decrypting analog data entered via a microphone.

17. The device of claim 1 configured as a secure voice recognition device, wherein said processing means comprises an electronic device capable of encrypting/decrypting data received via at least one of synchronous and asynchronous communication signals, serial clock and data signals, and computer bus signals.

18. The device of claim 1 configured as a secure voice recognition device including an interface to a Smartcard component as an integral part of the device, wherein said processing means comprises an electronic device capable of encrypting/decrypting and storing data via an algorithm contained on said Smartcard.

19. The device of claim 1 configured as a secure voice recognition device including an interface to a Smartcard component as an integral part of the device, wherein said processing means comprises an electronic device capable of encrypting/decrypting and storing data via said Smartcard..

20. The device of claim 1 configured as a secure voice recognition device including an interface to a Smartcard component as an integral part of the device, wherein said processing means comprises an electronic device capable of encrypting/decrypting and storing data via manipulation of commands in a command interpreter on said Smartcard.

21. The device of claim 1 configured as a secure voice recognition device including an interface to a Smartcard component as an integral part of the device,

wherein said processing means comprises an electronic device capable of preventing unauthorized use of software programs.

22. A method of providing secure data entry in a computer system, said method comprising the steps of:

performing at least one of entry, collection and reading of data information via a standard data entry device including a computer mouse, keyboard, voice system and the like,

encoding said data information within said standard data entry device for presentation to the computer system, and

processing, within said standard data entry device, said encoded data information by performing thereon at least one operation amongst operations including encryption, decryption, data manipulation and non-volatile storage,

said processed encoded data information providing a secure transaction when transmitted within the computer system, and when decrypted and decoded for use at a remote location.

23. A secure data entry peripheral device in a computer system, substantially as described herein by way of example and with reference to the drawings.

24. A method of providing secure data entry in a computer system, substantially as described herein by way of example and with reference to the drawings.

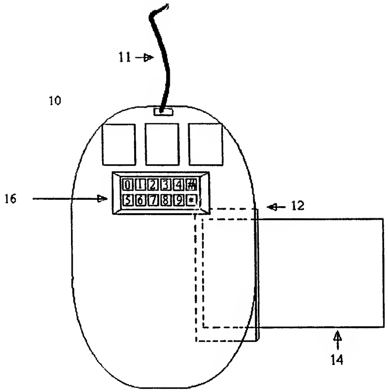


FIG. 1

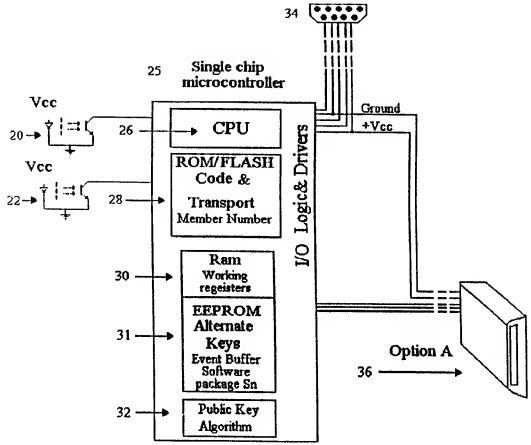


FIG. 2

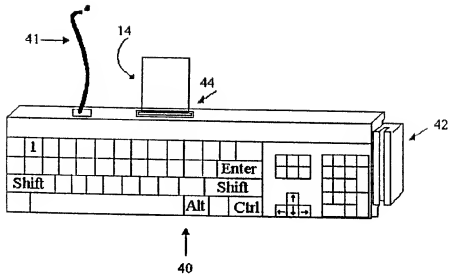


FIG. 3

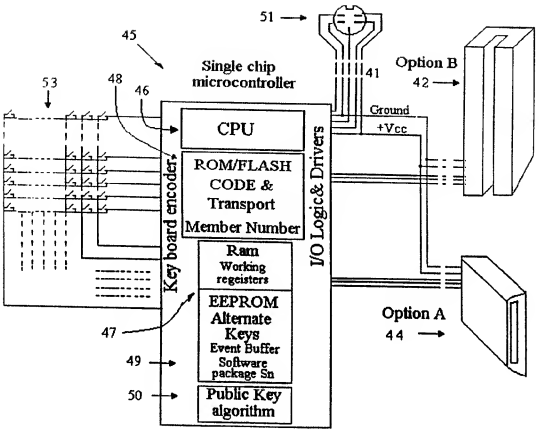


FIG. 4

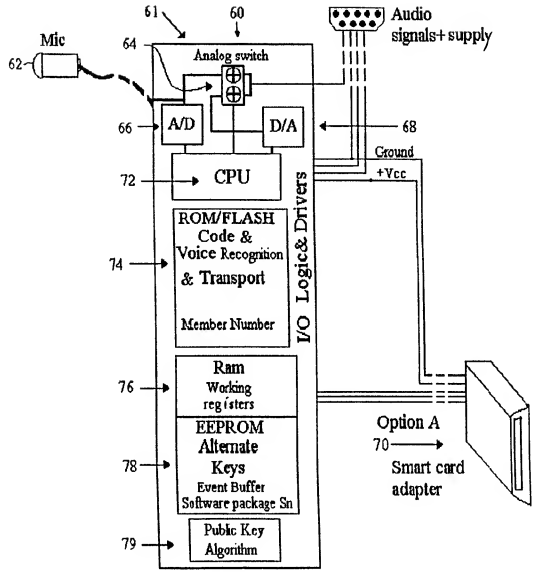


Fig. 5

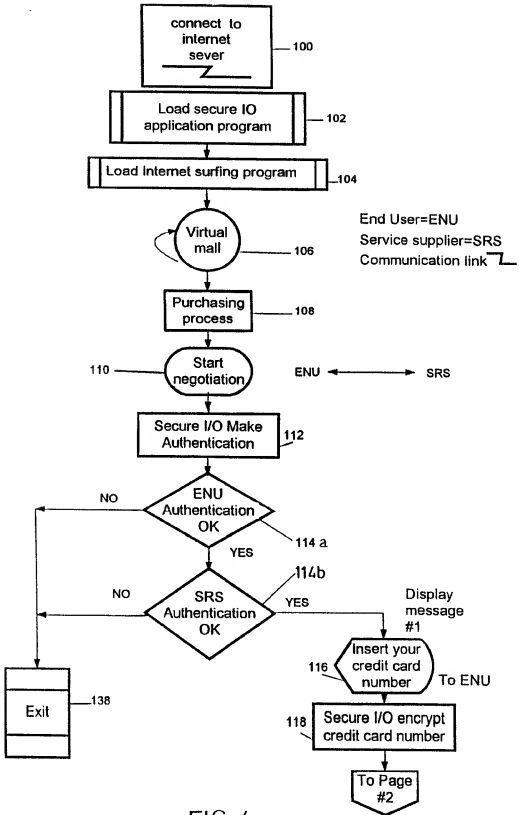


FIG. 6a

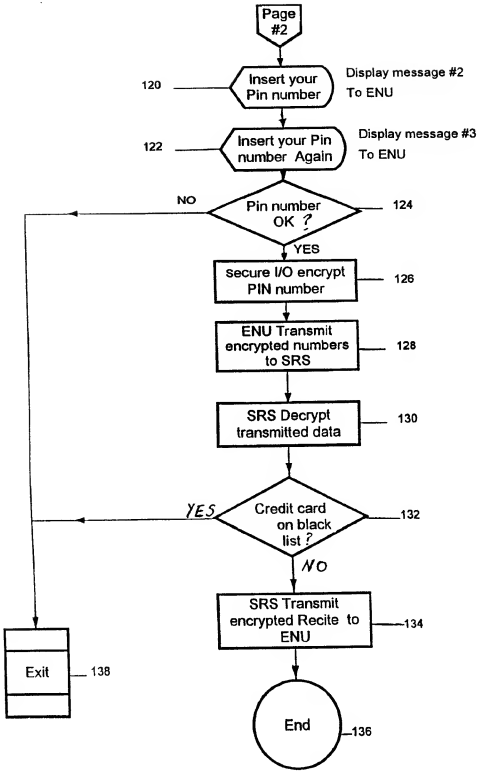


FIG. 6b

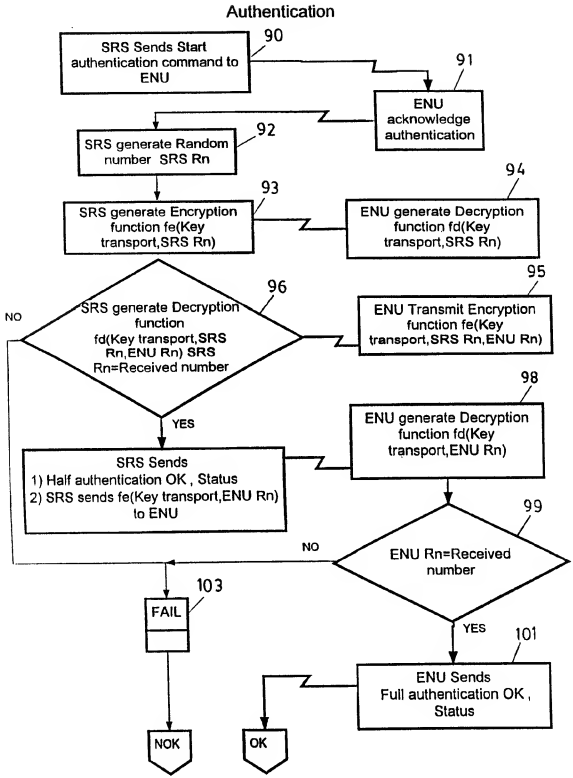


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL99/00504

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 12/14
US CL : 713/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E ---- Y,E	US 5,987,155 A (DUNN et al.) 16 November 1999, col. 6, line 3 - col. 7, line 2.	1,16-20, 22 ---- 2-15,21
Y	Secure Mouse for Internet. IBM tech. dis. bull. December 1997. Vol 40. No. 12. page 27	2-9
Y	US 5,596,718 A (BOEBERT et al.) 21 January 1997, col 4 line 27 - col 6 line 13	9,15,21
Y	US 5,605,406 A (BOWEN) 25 February 1997, col 5 line 21 - col 12 line 43	1-22

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 13 JANUARY 2000	Date of mailing of the international search report **14 FEB 2000**
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Joseph Palys Telephone No. (703) 308-7090

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL99/00504

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,745,055 A (REDLICH et al.) 28 April 1998, col. 5, line 51 - col. 6 line 11	7
Y	US 5,809,143 A (HUGHES) 15 September 1998, col. 2 line 51 - col. 12 line 18	1-22
Y	US 5,748,888 A (ANGELO et al.) 05 May 1998, col. 3 line 33 - col. 8 line 67	11
Y	US 5,742,758 A (DUNHAM et al.) 21 April 1998, col. 7 line 3 - col. 8 line 52	12
Y	US 5,359,660 A (CLARK et al.) 25 October 1994, col. 3 lines 3-26	13
Y	US 5,305,384 A (ASHBY et al.) 19 April 1994, col. 9 line 56 - col. 15 line 68	16-21

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL99/00504

Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 23 and 24
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

the specific invention claimed by each of claims 23 and 24 is unclear. See PCT rule 5.

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4 ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

IBM Technical Disclosure Bulletin, IEEE electronic library
search terms: secure mouse
WEST
search terms: secure mouse, secure keyboard, voice recognition, smart card, non-volatile memory, security, encode, encrypt, decrypt, data manipulation, process, peripheral, asynchronous